DOJ Component:FBI
Total Number of Federal Employees Component-wide: 35,119
Total Number of Contract Employees Component-wide: 11,103

Department of Justice
Self-Inspection Checklist

Document Security

A. Original Classification

(Section A applies only to components with Original Classification Authority [OCA])
Note. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

1. Does OCA training on the requirements and overall process cover the following:

- Applicable standards and categories for classification? ◉ Y ○ N ○ N/A
- Levels of classification and damage criteria associated with each? ◉ Y ○ N ○ N/A
- Avoidance of over-classification? ◉ Y ○ N ○ N/A
- Classification prohibitions and limitations? ◉ Y ○ N ○ N/A
- Required markings, including those for dissemination and handling? ◉ Y ○ N ○ N/A
- Obsolete/invalid markings? ◉ Y ○ N ○ N/A
- Determination of declassification instructions? ◉ Y ○ N ○ N/A
- Delegations of OCA responsibilities? ◉ Y ○ N ○ N/A
- Classification challenges? ◉ Y ○ N ○ N/A

1a. If **NO** to any of the above requirements and processes, please explain so appropriate education and training tools may be provided. **Click here to enter text.**

2. Do current OCAs have a demonstrable and continuing need to exercise this authority? ◉ Y ○ N ○ N/A

2a. If **YES**, please explain why OCAs have a demonstrable and continuing need.

(U) The FBI's 17 OCAs have a demonstrable and continuing need to exercise original classification authority. OCAs compose and authorize classification guides specific to their area of subject matter expertise in order to facilitate classification decisions for the different types of information (i.e., intelligence, continuity of operations, information assurance) encountered by the FBI. Additionally, the OCAs exercise their authority to facilitate declassification decisions, to share information with our Intelligence Community (IC) and Law Enforcement partners, and to use in legal proceedings.

3. Have OCAs prepared, as appropriate, classification guides to facilitate the proper and uniform derivative classification of information? ◉ Y ○ N ○ N/A

3a. If **NO**, please elaborate why classification guides have not been prepared.
Click here to enter text.

4. Do OCAs creating their own classification guides or contributing to an existing classification guide meet the requirements of Executive Order (EO) 13526, Section 2.2, and 32 Code of Federal Regulations (CFR) Part 2001, Section 2001.15? ◉ Y ○ N ○ N/A

4a. If **NO**, please explain why classification guides do not meet the above requirements.
Click here to enter text.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.

(U) The FBI currently has six classification guides.

B. Derivative Classification

(Section B applies only to components with persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide)

Note. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

5. Does derivative classification training on the process and requirements for derivative classification markings cover the following:

- Identity of derivative classifier? ◉ Y ○ N ○ N/A
- Use of source documents, including classification guides? ◉ Y ○ N ○ N/A
- Declassification instructions? ◉ Y ○ N ○ N/A
- Proper application of markings? ◉ Y ○ N ○ N/A
- Portion marking and overall classification marking? ◉ Y ○ N ○ N/A
- Classification authority block properly identifying derivative classifiers? ◉ Y ○ N ○ N/A
- Obsolete/invalid markings on source documents? ◉ Y ○ N ○ N/A
- Multiple sources identified? ◉ Y ○ N ○ N/A
- Classification challenges? ◉ Y ○ N ○ N/A

Click here to enter supporting text.

5a. If **NO** to any of the above requirements and processes, please explain so appropriate education and training tools may be provided.
Click here to enter text.

6. Do persons who apply derivative classification markings observe original classification decisions and carry classification markings forward to newly created documents? ◉ Y ○ N ○ N/A

7. Describe the process followed when derivative classifiers identify improper markings on an originally or derivatively classified document. Include actions taken or planned to correct deficiencies or misclassification actions and to deter their reoccurrence.

(U/~~/FOUO~~) Anyone who wishes to challenge the classification of FBI information may either proceed informally by directly questioning the classifier or they may submit a formal classification challenge. Those who wish to challenge the classification of other government agency (OGA) information must submit a formal classification challenge. Informal classification challenges may be invoked for derivatively classified FBI information; this includes documents marked "Classified" by an OCA or classification decisions rendered in a classification guide. All classification decisions pertaining to OGA information must be formally challenged. Informally challenged information remains marked at the level it was originally classified, but must be handled and protected at the

highest level of classification of the conflicting opinions until the classification conflict is resolved.

(U//~~FOUO~~) When uncertainties exist over the classification status of derivatively classified information, holders of this information are encouraged to make direct contact with the derivative classifier to correct the classification prior to making a formal classification challenge. Informal classification challenges do not require intervention by Security Division (SecD). However, challengers may make an informal request to the Strategy, Policy, and Information Security Unit (SPISU), Mission Support Section (MSS), SecD, for guidance and resources to help resolve the dispute.

(U//~~FOUO~~) When approaching a derivative classifier with a classification challenge, the challenger should be prepared to justify the challenge by referencing with an OCA's classification determination as conveyed in a classification guide or a properly, accurately marked source document. After the challenger approaches the derivative classifier who originated the document or information, the derivative classifier may either accept the proposed classification correction or determine that the information should remain marked as is.

(U//~~FOUO~~) If the derivative classifier accepts the proposed classification correction, he must create a record copy of the corrected document and, to the most practical extent, notify all holders of the information that the corrected document must be used instead of the incorrectly classified document. The derivative classifier must also record the change, to include the derivative source for the classification, and maintain a record of the change with the file or record copy of the document.

(U//~~FOUO~~) If the derivative classifier determines that the information should remain marked as is, the individual who challenged the classification may not change the marking on the originator's document. If the individual who challenged the classification still believes the information is incorrectly classified and wants to ensure that the correct markings are placed on the originator's document, he can initiate a formal classification challenge.

(U//~~FOUO~~) Formal classification challenges may be invoked for both originally and derivatively classified information, regardless of agency of origination. Formal challenges are made by filling out the "FBI Formal Classification Challenge Form FD-1061" and submitting it to SPISU. This submission may be either electronic or hard copy. All attempts will be made to resolve challenges within 60 days of receipt by SPISU. If unable to resolve the challenge within 60 days, SPISU will acknowledge the challenge in writing and provide a revised resolution date. The written response will also advise that if a response is not provided within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision.

(U//~~FOUO~~) For challenges to derivatively classified information, SPISU will determine the

appropriate classification guide(s) and respective OCA(s) associated with the information. Then, SPISU will liaise with that OCA (or his subject matter expert designee) to determine the proper marking for the information. All decisions and historical information pertaining to the challenge will be recorded by SPISU.

(U//~~FOUO~~) For challenges to originally classified information, SPISU will liaise with the OCA who made the decision, as well as any other applicable OCAs (or their subject matter expert designee), to determine the proper classification of the information. The OCA who originally classified the information in question will make the final classification decision.

(U//~~FOUO~~) For challenges to the classification of information originated an OGA, SPISU will liaise with the proper point of contact to determine proper classification of the information. All decisions and historical information pertaining to the challenge will be recorded by SPISU and a final classification decision will be rendered and conveyed, and SPISU will complete the FBI Formal Classification Challenge Form FD-1061.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

C. Classified Markings Review

(Regular reviews of representative samples of the component's original and derivative classification actions shall be conducted in accordance with 32 CFR Part 2001, Section 2001.60[c][2] to evaluate the classification and marking of the documents and electronic communications. These samples must encompass all component activities that generate classified information.)

8. How often is a sampling of original and derivative classification actions reviewed? (If **Other**, please explain.)

○ Monthly ○ Semi-annually ◉ Annually ○ Other ○ **N/A**

Click here to enter text.

8a. Identify what factors are considered in establishing time frame.

(U) All documents that were reviewed were created within Fiscal Year (FY) 2013. The FBI reviewed an assortment of electronic communications (ECs), emails, and intelligence information reports (IIRs). Every document reviewed was classified at the confidential or secret level. The reviews ensured that

basic requirements (i.e. banner line, portion marking, classification blocks and foreign dissemination markings) were required. For this exercise, reviewers did not challenge the classification level of portions deferring to the author's subject matter expertise unless the portion was blatantly over classified.

9. Identify number of original and derivative actions reviewed as a representative sample. A specific number must be provided for the various items reviewed, e.g., originally classified hard copy documents, originally classified e-mails, derivatively classified hard copy documents, derivatively classified e-mails, etc.

(U) 11 original actions and 189 derivative actions were reviewed. The 11 original actions, were all hard copy documents. Of the 189 derivative actions, 63 derivatively classified ECs, 61 derivatively classified IIRs/Intelligence Products, and 65 derivatively classified emails were reviewed.

9a. Are classified documents properly marked, to include documents containing Foreign Government Information, in accordance with the Information Security Oversight Office December 2010, Marking Classified National Security Information Marking Book or agency specific marking guide? ◉ Y ○ N ○ N/A

9b. In how many classified items sampled were discrepancies noted? Provide numbers for the specific items reviewed.
(U) 98

9c. List types and number of discrepancies identified during review **(see Attachment 1)**. Identify the types and number of discrepancies with the specific type of item reviewed.

(U) 39 Classified By Line- Derivative Classifier discrepancies, 30 Derived From Line discrepancies, 19 Portion Marking discrepancies, and 8 Multiple Sources discrepancies were identified during the review.

9d. Describe actions taken or planned to correct the discrepancies identified above.

(U) The primary cause of the referenced discrepancies can be grouped into two categories:

1) Classification Management Tool – The Classification Management Tool (CMT) is deployed on several FBI platforms including Microsoft Applications (including Outlook) and Sentinel (official system of record). Currently, there are inconsistencies among versions of the CMT because there are multiple versions of the CMT running across the enterprise. SecD is working with Information Technology Engineering Division to get the same updated version of the CMT deployed throuhgout

the FBI.

2) User Errors - To reduce and mitigate errors, the FBI continues to provide training awareness on correct classification marking and handling procedures to all FBI personnel. During FY2013, the FBI has developed and launched web-based training for designating, marking, and handling classified information. This training was completed by over 96% of FBI personnel. In addition, the FBI also provided in-person training to 1,133 persons. The FBI is finalizing a more in-depth training intended for the personnel with a more complex understanding of classified information.

(U) The FBI published 14 Security Bulletins in FY2013. Security Bulletins are intended to notify FBI personnel of new resources available to them such as the publication of a new classification guide or to provide awareness of common marking errors as necessary to correct the trend.

9e. How many actions reviewed were derivatively classified? Specify number of hard copy documents, e-mails, etc.

(U) 189 derivative actions were reviewed. Of the 189 derivative actions, 63 derivatively classified ECs, 61 derivatively classified IIRs/Intelligence Products, and 65 derivatively classified emails were reviewed.

1. What percent of derivatively classified actions contained derivative classifier's name and position, or personal identifier? Specify percentage of hard copy documents, e-mails, etc.
(U) 79%

9f. How many derivatively classified actions reviewed were derived from multiple sources? Specify number of hard copy documents, e-mails, etc.
(U) 8

1. What percent of the documents had a list of sources included or attached?
(U) 0%

EXPLANATORY COMMENTS: Use the space provided to elaborate on questions within this section. Click here to enter text.

D. Security Education
(OCAs are required to receive training in proper classification and declassification each calendar year.)

Note. If SEPS provides the services for your component, a comment box is provided at the end of the section for further elaboration.

10. How many OCAs exist within the component? (U) 17

10a. What percentage of OCAs received initial OCA training prior to originally classifying information? (U) 100%

10b. What percentage of OCAs have received annual OCA refresher training? (U) 100%

10c. Have any waivers to this requirement been granted? (U) No

(Derivative classifiers are required to receive training in the proper application of the derivative classification principles of EO 13526 each calendar year. A derivative classifier is anyone with a clearance as he/she has the potential to access and derive classified information.)

11. How many derivative classifiers exist within the component? (U) 46,222

11a. What percentage of derivative classifiers have received initial derivative classification training prior to derivatively classifying information? (U) 100%

11b. What percentage of derivative classifiers have received annual refresher training? (U) 96.4%

11c. Have any waivers to this requirement been granted? (U) No

(All cleared personnel are required to receive initial training on basic security policies, principles, practices; and criminal, civil, and administrative penalties. Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information [National Security Information/Sensitive Compartmented Information]. Cleared personnel who leave the Department or whose clearance has been withdrawn or revoked is required to receive a termination briefing.)

12. How many cleared federal employees exist within the component? (U) 35,119

12a. What percentage of cleared federal employees receive initial training?
(U) 100%

12b. What percentage of cleared federal employees receive refresher training?
(U) 96.4%

13. How many cleared federal employees left the Department or had a clearance withdrawn or revoked in the past year? (U) 1262

13a. What percentage of these cleared federal employees received a termination briefing? (U) 100%

14. Are authorized couriers of classified information briefed on their responsibilities? ◉ Y ○ N ○ N/A

15. Are records kept of the various training and briefings provided (initial/refresher/termination/courier) and the employees who participated? ◉ Y ○ N ○ N/A

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.

(U) The FBI Corporate Policy Directive 0192D, "Personnel Security Clearance and Access Policy," states that all personnel must be debriefed when they no longer require access to FBI information, including national security information; facilities; and information technology systems. Chief Security Officers (CSOs) ensure that all personnel are debriefed per FBI Corporate Policy Directive 0192D.

E. Declassification

(Section E applies only to components that create/maintain classified permanent records designated as such through an approved records schedule.)

Note. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

16. Does your component create/maintain classified permanent records designated as such through an approved records schedule? ◉ Y ○ N ○ N/A

17. Describe the process and procedures for how your component accomplishes declassification reviews of your classified permanent records. If your component works directly with SEPS to assist with your automatic declassification reviews,

please state that.

(U) The FBI's approach to automatic declassification is to first evaluate information at the file series level. File series exemptions are sought for file series that are national security related and the oldest information in the file series is at least 25 years old. When a file series exemption is granted, the information undergoes a review pursuant to the systematic declassification review provisions of Executive Order 13526 (see answer 18a). Classified FBI information residing in non-national security related file series, as well as other file series that do meet the criteria for a file series exemption, is automatically declassified without review when the information reaches 25 years of age.

18. Do approved exemptions from automatic declassification listed in the DOJ Automatic Declassification Guide (or ISCAP approved declassification guide (FBI) apply to classified permanent records your component creates/maintains?

◉ Y ○ N ○ N/A

18a. If **YES**, Describe the process and procedures for how your component accomplishes systematic reviews of your exempt classified permanent records. If your component works directly with SEPS to assist with your systematic declassification reviews, please state that.

(U) The FBI's Record/Information Dissemination Section (RIDS) is responsible for declassification reviews under the systematic declassification provisions of Executive Order 13526. While conducting these reviews, RIDS ensures information that no longer meets the criteria for classification established by the FBI Automatic Declassification Guide (ADG) is declassified and information that continues to meet the criteria for exemption from automatic declassification remains classified.

The FBI's ADG contains a list of exempt file series that require systematic review. When prioritizing the review of each exempt file series, RIDS considers factors such as the expiration date of the exemption, the size of the file series in relation to the expiration date of the exemption, historical significance, the organizational priorities of the Records Management Division and FBI management, and priorities (if any) established by the National Declassification Center.

During systematic declassification reviews each classified record is evaluated using the following process:

- Determine the originator of the classified information.
  - o Classified information which originates with another agency is tabbed using a Standard Form (SF) 715 to indicate that the information must be forwarded to the originating agency so that it can make a classification determination on its information.
- Determine the age of the information.
  - o When FBI classified information is between 25 and 50 years of age, all of the exemption codes listed

in the ADG are eligible to be applied. RIDS reviewers will seek to determine whether the classified information under review fits into any of the specific exemption codes.

-Classified information which, pursuant to the ADG, is exempt from automatic declassification is tabbed using a SF-715 to indicate the exempt status of the information.

-Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from automatic declassification is declassified.

o When the FBI classified information is 50 years of age, the review is limited to an evaluation as to whether the information is eligible for exemption from automatic declassification pursuant to portions of the ADG which implement Section 3.3(h)(2) of Executive Order 13526.

-There are only three categories of information that can be considered for exemption from automatic declassification at 50 years of age:

- The identity of a confidential human source or human intelligence source;
- Key design concepts of weapons of mass destruction; and
- "Extraordinary cases."

-Classified information which, pursuant to the ADG, is exempt from automatic declassification at 50 years of age is tabbed using a SF-715 to indicate the exempt status of the information.

-Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from automatic declassification is declassified.

19. Describe your component's procedures for mandatory declassification review requests received from the public.

(U) The following procedures are followed upon receipt of a Mandatory Declassification Review (MDR) request from the public:

- Data about the request is entered into the RIDS electronic case management and redaction system (i.e., FDPS).
- Using the criteria established in Executive Order 13526 and its implementing directives, the request is reviewed to determine whether it is a valid MDR.

o If it is determined that the MDR is not valid, RIDS will provide the requester, in writing, with the reason(s) for the denial of the MDR and an opportunity to modify the request or provide the information necessary for the request to be processed. Additionally, RIDS will notify the requester of the right to appeal the denial decision.

- Upon verification that RIDS possesses a valid MDR request, a search is conducted for records containing the information sought in the request.

o If no record is found, the requester is advised of this in writing and the requester is advised of his right to appeal this determination.

- When responsive records are located, RIDS performs a line-by-line declassification review of the information in accordance with applicable executive orders, regulations, policies, classification guides, or declassification guides.

o When information responsive to a MDR request originates with another agency and is in the possession of the FBI, RIDS will refer the information and the request letter to that agency. The receiving agency will communicate its determinations to RIDS. RIDS will then incorporate the other agency determinations into a final determination.

- For information that RIDS determines will be declassified, RIDS will mark or redact the information appropriately in FDPS to clearly designate that the information has been declassified. When information cannot be declassified in full, RIDS will make reasonable efforts to release the portions of requested information that constitute a coherent segment.
- Once the declassification review is complete, RIDS performs a separate line-by-line review for public release purposes, including a review to identify information that is exempt from disclosure under the provisions of a statutory authority, such as the Freedom of Information Act.
- The requester is then provided with the responsive documents and/or the reason(s) why information is being withheld or redacted, including citations to sections 1.4 or 3.3 of Executive Order 13526 or other specific legal authorities. The requester is also notified of his appeal rights.

(Mandatory declassification review requests apply to both classified permanent and temporary records. If you are unfamiliar with mandatory declassification reviews, contact your FOIA section as they are usually the section that would initially receive these requests.)

20. Does your component have a process for facilitating public release or access of declassified documents, e.g., FOIA Electronic Reading Rooms, FBI Vault. ◉ Y ○ N ○ N/A

20a. If **YES**, please describe.

(U) The mission of the FBI's RIDS is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and information. The requests and disclosures comply with the Freedom of Information and Privacy Acts (FOIPA), Title 5, United States Code, Sections 552 and 552a; the MDR and systematic review provisions of Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and other Presidential and Congressional directives. RIDS efforts are directed to appropriately release information in an efficient and effective manner while protecting legitimate law enforcement, foreign policy, national security, and defense interests.

(U) To date in FY2013, the FBI has received approximately 18,965 FOIPA and other access requests from the public. RIDS has reviewed at least 1.29 million pages pursuant to these requests. FOIPA and other requests are processed in FDPS, an electronic case management and redaction system, which promotes the efficient processing and release of declassified non-exempt information to the public. In late FY2013 a new version of FDPS was deployed which will allow for even more efficient processing and disclosure of declassified non-exempt information to the public in FY2014. RIDS can respond to requesters in

either paper or electronic formats.

(U) To facilitate public access to declassified and other non-exempt information, RIDS maintains a public website known as "The Vault." Thus far in FY2013, "The Vault" has received 4,896,504 views. The website contains approximately 3.7 terabytes of historically significant information on 520 different subject matters. The accessibility of information on "The Vault" continues to receive a significant amount of positive feedback from the requester community, the media, and the general public.

(U) Thus far in FY2013, RIDS has conducted declassification reviews on nearly 1.2 million pages of permanently valuable classified records 25 years of age and older pursuant to the systematic declassification provisions of Executive Order 13526. Nearly all of these pages will be transferred to the National Archives where they will undergo further processing for eventual availability to the public.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

F. Safeguarding
Note. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

21. Is all classified material properly protected in accordance with 32 CFR Part 2001.Subpart D and the Department of Justice (DOJ) Security Program Operating Manual (SPOM), Chapter 6?

- Do you have a system of control measures which assures access to classified information is limited to authorized persons? ◉ Y ○ N ○ N/A
- Do you have a system of control measures which deter and detect access by unauthorized persons? ◉ Y ○ N ○ N/A
- Is classified material stored in General Services Administration (GSA) approved security containers or Department Security Officer (DSO) approved open storage areas? ◉ Y ○ N ○ N/A
- Is Top Secret information stored in a GSA-approved security container along with proper supplemental controls? ◉ Y ○ N ○ N/A
- Are combinations safeguarded the same as the highest level of classified information being protected? ◉ Y ○ N ○ N/A

- Are combinations changed only by persons authorized access to the highest level of information stored in the container? ◉ Y ○ N ○ N/A
- Do you use Standard Form (SF) 700s "Security Container Information"? ◉ Y ○ N ○ N/A
- Do you have Confidential or Secret information protected by a key operated lock? ○ Y ◉ N ○ N/A

- Is classified information kept under constant surveillance and covered to prevent unauthorized access when removed from storage for working purposes? ◉ Y ○ N ○ N/A
- Is a system of security checks or inspection implemented at the close of each business day to ensure classified information is properly secured? ◉ Y ○ N ○ N/A
  - Are SF 702s "Security Container Check Sheets" utilized? ◉ Y ○ N ○ N/A
  - Are SF 701s "Activity Security Checklist" utilized? ◉ Y ○ N ○ N/A
- Does the official responsible for arranging a conference or meeting institute ensure adequate security is provided if classified information is to be discussed? ◉ Y ○ N ○ N/A
  - Are meetings held only in a U.S. Government facility or at a cleared facility of a DOJ contractor or consultant? ◉ Y ○ N ○ N/A
  - Are attendees notified of imposed security limitations due to attendees' access level authorizations or physical security conditions of the facility? ◉ Y ○ N ○ N/A

22. Is all classified material transmitted in accordance with 32 CFR Part 2001, Section 2001.45 and the DOJ SPOM, Chapter 6-500?

- Is classified information physically transmitted outside the facility in two opaque layers? ◉ Y ○ N ○ N/A
- Is authorization to hand-carry classified information between DOJ components and other organizations only given to DOJ personnel ◉ Y ○ N ○ N/A

appropriately briefed and authorized in writing by the SPM?

23. Is all classified material reproduction in accordance with 32 CFR Part 2001, Section 2001.44 and the DOJ SPOM, Chapter 6-402?

- Held to a minimum consistent with operational requirements? ◉ Y ○ N ○ N/A
- Accomplished only by authorized persons knowledgeable of the procedures for classified reproduction? ◉ Y ○ N ○ N/A
- Accomplished only with approved equipment? ◉ Y ○ N ○ N/A
- Appropriate procedures for reproduction of classified information posted on or near equipment approved for such reproduction? ◉ Y ○ N ○ N/A

24. Is all classified material destroyed in accordance with 32 CFR Part 2001, Section 2001.46 and the DOJ SPOM, Chapter 6-600? ◉ Y ○ N ○ N/A

If **NO** to **21-24**, please explain further.

(U) The FBI uses X-09 combination locks on all containers used to store classified information.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

G. Telecommunications, Automated Information Systems (IT), and Network Security
Note. If SEPS provides the services for your component, a comment box is provided at the end of the section for further elaboration.

25. Consistent with EO 13526, Section 4.1; 32 CFR Part 2001, Section 2001.50; and the DOJ SPOM, Chapter 8, describe uniform procedures established to ensure automated information systems that collect, create, communicate, compute, disseminate, process or store classified information are protected in accordance with applicable national policy issuances.

(U) The FBI Certification and Accreditation (C&A) process supports the goal of the FBI Information Assurance Program to protect national security information and information systems processing that

information. In order to attain this goal, the FBI's Information Assurance (IA) Program includes elements that:

• Ensure all individuals with access to classified or sensitive information [e.g. For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES)] or FBI information systems that process classified or sensitive information have the proper security clearance, formal accesses, need to know, and training.

• Ensure the confidentiality, integrity, and availability of information processed by FBI information systems

• Protect the FBI enterprise through the infusion of security technology and appropriate oversight.

• Establish a comprehensive, consistent, and centrally managed IA Program that institutes full lifecycle security.

(U) The FBI implements the security authorization process, as defined in the C&A Handbook, to determine information systems' compliance with the goals stated above and the controls outlined in the Information System Security Framework Policy. This policy defines the minimum baseline information systems security controls to ensure that the confidentiality, integrity, and availability of the FBI's computer systems, networks, and information are maintained. These information assurance standards, including those contained in the associated appendices of the Information Systems Security Framework Policy, are used to consistently identify and to select applicable security controls to secure FBI information systems based on assessed risks.

26. Describe procedures implemented to prevent unauthorized access, ensure the integrity of the information, and maximize the accessibility of information to persons who meet the criteria set forth in EO 13526, Section 4.1(a).

(U) The FBI C&A process supports the IA Program's efforts to protect national security information and the information systems processing that information. In order to attain this goal, the FBI's IA Program includes elements that:

• Ensure all individuals with access to classified or sensitive information (FOUO, SBU, LES) or FBI information systems that process classified or sensitive information have the proper security clearance, formal accesses, need to know, and training.

• Ensure the confidentiality, integrity, and availability of information processed by FBI ISs.

• Protect the FBI's Enterprise through the infusion of security technology and appropriate oversight.

• Establish a comprehensive, consistent, and centrally managed IA Program that institutes full lifecycle security.

(U) The FBI implements the security authorization process, as defined in the C&A Handbook, to determine information systems' compliance with the goals stated above and the controls outlined in the Information System Security Framework Policy. This policy defines the minimum baseline IS security controls to ensure that the confidentiality, integrity, and availability of the FBI's computer systems, networks, and information are maintained. These information assurance standards, including those contained in the associated appendices of the Information Systems Security Framework Policy, are used to consistently identify and to select applicable security controls to secure FBI information systems

based on assessed risks.

27. Do all IT systems that process, store, or handle classified information meet the requirements in the DOJ SPOM, Chapter 8? ◉ Y ○ N ○ N/A

27a. If **NO**, please explain. **Click here to enter text.**

28. Are all IT system components having the potential to retain classified information marked with the highest classification level and most restrictive classification category? ◉ Y ○ N ○ N/A

28a. If **NO**, please explain. **Click here to enter text.**

29. Is all data introduced on a classified IT system the same or lower security classification level for which the IT system is approved to operate? ◉ Y ○ N ○ N/A

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

H. Security Violations
(All security violations are required to be reported to the Department Security Officer.)

30. Is the loss, possible compromise, or unauthorized disclosure of classified information appropriately reported in accordance with the DOJ SPOM, Chapter 1-300? ◉ Y ○ N ○ N/A

30a. Are personnel familiar with the reporting procedures? ◉ Y ○ N ○ N/A

30b. What procedures are implemented to conduct an inquiry/investigation?

(U) The Security Compliance Unit (SCU), MSS, SecD, oversees and manages the FBI's Security Incident Program by ensuring that all reported incidents are documented, investigated and mitigated. When an employee or personnel associated with the FBI (e.g., contractors, task member) has committed or becomes aware of a security incident, he reports the incident to his respective CSO. CSOs are then responsible for reporting the security incident to SCU via the FBI's Security Incident Reporting System (SIRS). CSOs are responsible for conducting an inquiry into each incident that occurs within their division to ensure that all security concerns are resolved.

30c. Are appropriate and prompt corrective actions taken when a security violation or infraction occurs? Describe process. ◉ Y ○ N ○ N/A

(U) Yes. SIRS is the FBI's central database used to capture all security incidents reported by employees and personnel associated with the FBI (e.g., contractors, taskforce members). Upon receipt of an incident, SCU personnel work closely with CSOs and other security professional as well as other entities as needed to ensure the incident is properly investigated/mitigated. As part of the mitigation process, CSOs are held responsible for conducting awareness briefings and providing training on security policy and procedures to individuals who commit security incident; this is intended to help prevent future occurrences. In addition, all parties with a vested interest in reported security incidents are notified. For example, referrals are made to:

- Initial Processing Unit - potential misconduct
- Privacy & Civil Liberties Unit - potential breach of personnally identifiable information
- Counter intelligence - potential espionage matters
- Enterprise Security Operations Center - information technology incidents
- Strategy, Policy, & Information Security Unit, SecD – federal taxpayer and information security incidents

(U) In July 2013, SCU implemented the Critical Incident Notification tool to ensure timely reporting of high-risk security incidents to SecD Executive Management.

30d. Are individuals who commit violations or infractions subject to appropriate sanctions? ◉ Y ○ N ○ N/A

EXPLANATORY COMMENTS: Use the space provided to elaborate on questions within this section. Click here to enter text.

I. Management and Oversight

Note. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

31. How many personnel are dedicated to manage the classified national security information program? (U) 18

32. Are sufficient resources and personnel committed to implement the classified national security information program? If **NO**, please explain. ○ Y ◉ N ○ N/A

(U) More dedicated personnel and funding for travel are required to provide more customized training across the FBI's 56 field divisions. The current restrictions on travelling to field divisions limits SecD's

ability to conduct thorough onsite reviews and self inspections of the FBI's classification management capabilities. The FBI's ability to conduct thorough document reviews is also limited.

33. Describe how security personnel fulfill responsibilities to implement the program.

(U) Through the implementation of policies and proceedures based on guidance form EO 13526.

(The performance contract or other rating system of OCAs, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information.)

34. How many personnel fit within the categories identified above?
(U) 9

34a. What percentage of such personnel at your component has this element in their performance contracts? (U) 0%

35. How many cleared contract employees exist within the component world-wide?
(U) 11,103

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

Please include the following information in your report to the Department Security Officer on the results of your self-inspection:

1. A description of the component's self-inspection program to include the criteria identified below. The description should demonstrate how the self-inspection program provides the senior agency official with information necessary to assess the effectiveness of the classified national security information program within the component as a whole (Headquarters/ Division/District/Field/Resident/Satellite/Overseas offices).

    - Who conducts the self inspections;
    - Activities assessed;
    - Program areas covered; and
    - Methodology utilized.
        - Means and methods employed;

- Different types of self inspections conducted (interviews with producers and users of classified information, reviews of representative samples).
- Include how component headquarters gather information from the various offices, e.g., Division/District/Field/Resident/Satellite/Overseas offices.

(U) The Information Security Oversight Program (ISOP) is located in SPISU. ISOP is responsible for all information security reporting required by agencies outside for the FBI, and also conducts document reviews for these reports. Due to sequestration and limited travel funding, ISOP personnel conducted document reviews using a combination of Sentinel, which is theFBI's official system of record, and other databases and surveys of field and Headquarters CSOs.

(U) The review methodology consisted of seven individuals reviewing a random selection of ECs in Sentinel, IIRs from the Intelligence Portal, and classified emails from their own email boxes. The criterion for the review was not based on substantive classification. The documents were reviewed based on whether the documents had correct banner lines, portion markings, and declassification blocks. If discrepancies were consistent, an issue was identified for future action. Identified future actions included developing and disseminating security bulletins, developing training, and updating the classification tools on the computer application used to generate the document (i.e., CMT on Outlook).

Criteria included details regarding:

- Banner lines
- Portion markings
- Classification Authority Block
- Proper "Classified By" line
- "Derived from" line (if applicable)
- Declassification instructions
- List of sources (if applicable)
- Dissemination controls
- Markings uniformly and conspicuously applied

(U) The ISOP will continue to explore the use of the audit capabilities in Sentinel in future reviews to address a wider sample of FBI originating documents. The review was not intended to determine if the information is classified at the correct level, only to determine the presence and agreement of the basic elements of classification. The ISOP will conduct onsite reviews of documents when funding for travel becomes available. It is anticipated that between onsite reviews and available auditing capabilities of FBI information technology, a more representative sample of FBI generated classified documents will be obtained in future years.

2. Identify best practices that were identified during self-inspections.

(U) Best practices identified during the self-inspection include:

•Continue onsite reviews and document reviews using information technology system audit capabilities, such as Sentinel and CMT.

-The CMT is a commercial, off-the-shelf tool that works with most Microsoft Office products. It was originally created by the Central Intelligence Agency, and is compliant with all Controlled Access Program Coordination Office classification policies. A version is available on FBI's Sentinel and all FBI

Microsoft desktop applications. Currently, the FBI is working to ensure the same version of the CMT is deployed across all FBI applications, as well as to verify that all FBI classification guides are up to date and consistently cited in the CMT.

•The FBI has expanded it's training to meet the needs of differenet job roles within the component.

- The FBI's Working with Classified Information web-based training was launched in FY2013 to excellent reviews from FBI personnel. This training will become an annual requirement that will be able to satisfy the refresher training requirement for most FBI employees.

-The FBI has developed a "Working with Classified Information 201." This in-person class is intended for FBI personnel with a need for a more indepth understanding of classification rules and practices. Based on available funding, in-person training will continue in the field with recurring training at headquarters and other Washington, DC metro-area locations.

•The ISOP will continue to publish Security Bulletins on common information security errors and disseminate them to the entire FBI.

ATTACHMENT 1
EXPLANATION OF DISCREPANCIES

OVERCLASSIFICATION: (a) Clear-cut: The information in the document does not meet the standards necessary for classification; (b) Questionable: While the question of meeting classification standards is arguable, classification does not appear to be necessary to protect our national security; (c) Partial: A portion(s) of the document appear(s) to be unnecessarily classified, although the overall classification of the document is correct.

OVERGRADED: All or some of the information in the document appears to be classified at a higher level than justified.

UNDERGRADED: All or some of the information in the document appears to be classified at a lower level than necessary.

DECLASSIFICATION: The document has improper or incomplete declassification instructions or no declassification instructions.

The "Declassify on" line should contain one of the following:
(1) a date or event less than 10 years from the date the information/document was created;
(2) a date 10 years from the date the information/document was created;
(3) a date greater than 10 years and less than 25 years from the date the information/document was created;
(4) a date 25 years from the date the information/document was created;
(5) 25X1–25X9, with a date or event of declassification, provided that the classifying agency has received approval from the Interagency Security Classification Appeals Panel (ISCAP) to exempt the information;
(6) 50X1–50X9, with a date or event of declassification, provided that the classifying agency has received approval from the ISCAP to exempt the information;
(7) 50X1-HUM or 50X2-WMD, provided that the ISCAP has been informed of the agency's intent to use this marking; or
(8) 25X1, E.O. 12951, provided that the document contains space-based imagery.

Other markings, such as "OADR" and X1–X8, are not valid under the current Order, and "MR," "DCI/DNI Only," and "Subject to International Treaty or Agreement" have never have been valid declassification markings. See 32 C.F.R. Part 2001 and/or the ISOO booklet, "Marking Classified National Security Information," for further details.

When declassification dates are displayed numerically, the following format must be used: YYYYMMDD.

DURATION: A lesser duration of classification appears more reasonable.

UNAUTHORIZED CLASSIFIER (Unknown Basis for Classification): The document appears to have been classified by someone not authorized to do so.

"CLASSIFIED BY" LINE – Original Classification (Unknown Basis for Classification): The document does not identify the OCA by name and position or by personal identifier. If the identification of the originating agency or office is not apparent on the face of the document, it should be listed below the position.

"REASON" LINE: An originally classified document does not include the "Reason for Classification," or it cites an incorrect category from section 1.4 of the Order. A "Reason" line does not appear on a derivatively classified document, and if included is cited as a discrepancy.

"CLASSIFIED BY" LINE – Derivative Classification (Unknown Basis for Classification): The document does not identify the derivative classifier by name and position or by personal identifier.

ATTACHMENT 1
EXPLANATION OF DISCREPANCIES

"DERIVED FROM" LINE (Unknown Basis for Classification): The document fails to cite, or cites improperly, the classification source. The line should include type of document, date of document, subject, and office/agency of origin.

MULTIPLE SOURCES(Unknown Basis for Classification): The document cites "Multiple Sources" as the basis for classification, but does not list these sources.

ORIGINAL/DERIVATIVE: The document is marked and treated as an original classification action although the classified information appears to be derived from a guide or other source(s).

MARKING: The document lacks overall classification markings or has improper overall classification markings (e.g., lacks the highest overall marking, contains erroneous overall markings, or lacks overall markings and/or caveats on transmittal documents).

PORTION MARKING: The document lacks required portion markings.